

We claim:

1 1. A method for inoculating email infected with a virus, the email being
2 composed of data packets sent over a network and associated with a traffic flow in
3 the network, the method comprising:

4 scanning the data packets forming the traffic flow associated with the email;
5 detecting the signature of a known virus in the data packets;
6 determining whether there is an attachment associated with the email; and
7 altering bits of the data packet associated with the attachment in order to
8 inoculate the email.

1 2. The method of Claim 1 wherein altering the bits entails setting all the
2 bits associated with the data packet to a predetermined value.

1 3. The method of Claim 1 wherein the method is performed by a
2 content processor in a network device operating at wire speed.

1 4. The method of Claim 1 wherein the signature is detected in the text
2 of the email.

1 5. The method of Claim 4 wherein the signature is ASCII text.

1 6. The method of Claim 1 wherein the signature is a binary signature
2 located in the attachment.

1 7. The method of Claim 1 wherein the signature is stored in a memory,
2 the memory holding a database of known signatures.

1 8. The method of Claim 7 wherein a new virus signature is added by
2 loading the new virus signature into the database of new signatures.

1 9. The method of Claim 1 further comprising before scanning the data
2 packets, identifying the data packets as containing email.

1 10. A network device for scanning and inoculating email infected with a
2 virus, the email being composed of data packets sent over a network and associated
3 with a traffic flow in the network, the network device comprising:

4 memory storing a database of known signatures, the known signatures
5 including signatures of viruses;

6 a content processor connected to the memory, the content processor operable
7 to scan the data packets and determine whether the contents of the data packets
8 match one of the signatures of viruses in the database of known signatures, and to
9 determine whether the email associated with the data packets includes an
10 attachment, the content processor further operable to alter bits of the data packets
11 forming the attachment, thereby inoculating the attachment and the email.

1 11. The network device of Claim 10 wherein the content scanning engine
2 is able to scan across multiple data packets by storing intermediate conclusions in a
3 session memory.

1 12. The network device of Claim 10 wherein the content processor is
2 formed by a queue engine operable to reorder out of order data packets, a content
3 scanning engine operable to scan the data packets, and a context engine operable to
4 schedule data packets for scanning by the content scanning engine.

1 13. The network device of Claim 10 wherein the traffic flow is identified
2 by a unique session id.

1 14. The network device of Claim 10 further comprising a quality of
2 service processor connected to the content processor and operable to schedule the
3 transmission of the data packets onto the network.

1 15. The network device of Claim 10 wherein the content scanning engine
2 is able to match signatures of arbitrary length, scan across boundaries of the data
3 packets, and begin and end scanning anywhere within the data packet.

1 16. The network device of Claim 10 further comprising a host processor
2 in communication with the content processor, the host processor operable to
3 compile the database of known signatures and cause it to be loaded into the
4 memory.

1 17. The network device of Claim 16 wherein a new virus signature is
2 added by creating a new database of known signatures, recompiling the new
3 database in the host processor, and loading the new database of known signatures
4 into the memory.

5

1 18. The network device of Claim 16 wherein a new virus signature is
2 added by loading the new virus signature directly into the database of known
3 signatures.